Analisis Keamanan Jaringan Local Area Network yang Menggunakan DHCP Server Berbasis Cisco dengan metode Penetration Testing

Medianto
Program Studi Sistem Informasi, Universitas Internasional Batam
Jl Gajah Mada, Baloi Sei Ladi Batam 29442
E-mail: mediantolim8888@gmail.com

Abstract

The writing of this scientific paper aims to solve the problem of DHCP Rogue network attack method using DHCP Snooping which is a network security feature that is rarely used by people, because the lack of knowing the importance of network security causes the network to be given less attention on the security matter. For this reason, this scientific paper will discusses how to counteract DHCP Rogues with DHCP Snooping and how to implement these security features on the network. Apart from that, to prove whether using the DHCP Snooping feature is able to counteract Rogue DHCP attacks. The research method used by the author by conducting a study that uses simulation networks. Because of the author is using Cisco-based DHCP Snooping, the authors will conduct research where network simulation will be made in Cisco Packet Tracer simulation applications specifically for simulating with Cisco hardware. From the results of the comparison and conclusions of the study, the authors stated that ordinary networks that do not use the DHCP security feature of Snooping have the potential to be exposed to DHCP Rogue attacks. DHCP Rogue attacks causes hackers to be able to control the entire network by only spreading IP from hackers DHCP server to the network. On the other hand, networks that use the DHCP Snooping network security feature are able to completely ward off IP that is spread from hackers and the client only gets IP from the company's official DHCP Server, so the network is safe and protected from the control of hackers.

Keywords : DHCP Snooping, DHCP Rogue, Cisco Packet Tracer, how DHCP Snooping works, network security.

I. PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang semakin cepat menyebabkan banyak perusahaan beralih menggunakan jaringan komputer yang mampu mempermudah pembagian data dan informasi (Ariyadi, 2017). Dengan penggunaan jaringan komputer, mampu memberikan hasil yang lebih optimal dibandingkan dengan tidak menggunakan jaringan komputer.

Penggunaan jaringan komputer yang semakin banyak mengharuskan setiap komputer memiliki identitas masing-masing yang dikenal dengan *IP Address*. Setiap komputer dalam jaringan memerlukan indentitas tersebut agar mampu berkomunikasi antara satu komputer dengan yang lainnya. Identitas komputer dalam jaringan ini masing-masing akan diberikan secara

otomatis melalui *DHCP Server*. *DHCP Server* berperan untuk membagikan sejumlah alamat IP yang sebelumya telah dikonfigurasi yang kemudian dibagikan kepada komputer-komputer yang terhubung satu sama lain dengan *DHCP server*, sehingga admin jaringan tidak perlu mendaftar satu-persatu *IP Address* komputer dalam jaringan (Chen & Mao, 2015).

Seiring dengan penggunaan jaringan komputer yang semakin banyak dalam perusahaan, para peretas mulai memikirkan cara untuk mendapatkan informasi perusahaan melalui jaringan komputer ini. Untuk itulah diperlukan peningkatan keamanan jaringan komputer (Chen & Mao, 2015). Cara peretasan yang paling sederhana seperti penggunaan *DHCP Rogue*, dimana peretas menciptakan sebuah *DHCP server* imitasi yang dihubungkan dengan jaringan komputer utama perusahaan. Sehingga beberapa *client DHCP server* utama perusahaan akan mendapatkan *IP* dari *DHCP server* palsu yang dibuat dan alhasil tidak bisa terhubung ke jaringan perusahaan, melainkan terhubung dengan jaringan peretas (Miftah, 2018).

Apabila *DHCP Server* terserang *DHCP Rogue*, identitas dan koneksi imitasi yang disebarkan melalui *DHCP server* peretas sehingga client yang menerima IP dari server peretas akan dibelokkan koneksinya menuju ke jebakan peretas, semisal contoh, komputer *client* yang digunakan untuk mengakses data perbankan ataupun database perusahaan akan diketahui oleh peretas melalui trafik akses *client*, karena trafik yang dilalui *client* sudah dimanipulasi oleh peretas. Peretas hanya perlu mengumpulkan informasi mengenai akses situs sehari-hari *client*, dan kemudian melakukan *phising* situs-situs yang akan dibuka *client* untuk mendapatkan data *username* serta *password*. Masalah tersebut dapat terjadi karena adanya akses internet dalam jaringan perusahaan. Sehingga akar masalah tersebut akan dibahas dalam laporan karya ilmiah ini.

Untuk menganalisa dan mengantisipasi masalah keamanan jaringan komputer seperti yang penulis deskripsi diatas, penulis menggunakan teknik keamanan jaringan *DHCP Snooping*. *DHCP Snooping* merupakan sebuah teknik untuk mengamankan paket yang dikirm *DHCP Server* kepada *client* dan memastikan paket IP yang di *offer dan acknowledge* oleh client merupakan *DHCP server* yang berstatus terpercaya dari *server* perusahaan (Ariyadi, 2017).

Dengan latar belakang yang telah penulis jelaskan diatas, penulis akan melakukan analisis yang membandingkan jaringan komputer yang tidak menggunakan keamanan *DHCP snooping* dengan jaringan yang menggunakan keamanan *DHCP snooping* menggunakan aplikasi *Cisco Packet Tracer* untuk merancang simulasi jaringan komputer. Dengan ini, diharapkan pembaca mampu mengetahui secara langsung dampak yang terjadi apabila tidak mengimplementasikan keamanan dalam jaringan komputer dan bagaimana cara menindaklanjutinya. Untuk itu, penulis akan fokus membahas topik mengenai uraian diatas dengan judul karya ilmiah "ANALISIS KEAMANAN JARINGAN LOCAL AREA NETWORK YANG MENGGUNAKAN DHCP SERVER BERBASIS CISCO DENGAN METODE PENETRATION TESTING"

1.2 Tujuan Penulisan

Beberapa tujuan analisis dan penulisan karya ilmiah ini diuraikan sebagai berikut:

a) Mengetahui dampak yang akan terjadi apabila jaringan terserang *DHCP Rogue*
b) Mampu mengetahui cara kerja *DHCP Snooping* sehingga mampu menjalankan langkah preventif dari serangan peretas.
c) Mampu merancang sebuah keamanan jaringan dengan menggunakan teknik *DHCP Snooping*.

II. Tinjauan Pustaka

Keamanan pada jaringan mulai menjadi hal yang diprioritaskan perusahaan yang memiliki jaringan sendiri, seperti pada jurnal yang ditulis oleh Ariyadi pada tahun 2017 yang berjudul "Desain Keamanan DHCP Snooping untuk mengurangi serangan LAN" dimana penulis dalam jurnal tersebut bermaksud untuk membangun sebuah desain keamanan jaringan

untuk perusahaan dengan latar belakang dan tujuan agar semua pengguna jaringan yang menggunakan desainnya tersebut dapat merasa lebih aman dan terhindar dari serangan kejahatan *cyber* yang mampu dilakukan oleh pihak yang tidak bertanggung jawab.

Dalam jurnal yang ditulis oleh (Ariyadi, 2017) tersebut, menggunakan metode *DHCP Snooping* yang dimana dengan menggunakan metode ini, komputer yang terhubung jaringan serta menggunakan *DHCP Server* hanya dapat memberikan akses kepada IP yang sebelumnya telah terdaftar dalam *router* perusahaan dan komputer yang tidak memiliki IP yang terdaftar tidak mampu mengakses jaringan perusahaan.

Metode penulisan yang digunakan untuk menghasilkan jurnal ini menggunakan metode *experimental* dengan menerapkan simulasi yang telah ia buat dengan menggunakan *router mikrotik* sebagai *DHCP Server* dan beberapa komputer klien sebagai bahan simulasi *DHCP* klien. (Ariyadi, 2017) juga menggunakan *switch cisco* untuk konfigurasi *port* berstatus *Trusted* dengan arti sumber IP terpercaya sehingga klien *DHCP* tidak terbagi IP yang tidak dikenal selain dari yang didaftar oleh perusahaan. Konfigurasi dalam *switch cisco* juga melibatkan pembatasan *user (limit rate)* agar terhindar dari peretas yang tidak bertanggung jawab.

Kesimpulan yang didapat oleh (Ariyadi, 2017) dalam jurnal ini menuliskan bahwa *DHCP snooping* merupakan sebuah teknik atau metode keamanan yang msmpu menentukan *port* mana saja yang dipercaya untuk pembagian IP dari *DHCP server*, serta membatasi lalu lintas *DHCP* dari sumber-sumber yang *trusted* (terpercaya) dengan yang *untrusted* (tidak terpercaya) sehingga apabila perangkat peretas mencoba berinteraksi dengan cara mengirim paket *DHCP* ke dalam jaringan perusahaan, maka port akan otomatis tertutup dan mati.

Penulis sendiri berpendapat bahwa dari hasil jurnal diatas mampu meyakinkan pembaca bahwa penerapan keamanan jaringan mampu meminimalisir terjadinya hal yang tidak diinginkan perusahaan. Namun jurnal yang ditulis oleh (Ariyadi, 2017) tidak memaparkan data yang valid dan bukti yang kuat untuk membuktikan bahwa penerapan keamaman jaringan berpengaruh pada perusahaan. Untuk itu penulis akan menampilkan landasan teori selanjutnya dengan judul laporan "Simulasi keamanan jaringan dengan metode DHCP Snooping dan VLAN".

Pada jurnal yang ditulis oleh Zaeni Miftah pada tahun 2018 memiliki data hasil analisanya yang lengkap untuk membuktikan pengaruh keamanan jaringan. (Miftah, 2018) memiliki latar belakang untuk menawarkan sistem keamanan jaringan kepada STMIK Eresha karena banyaknya pengguna jaringan mulai dari pengakses pembelajaran online, akses sistem akademik, akses untuk perpustakaan online, sehingga (Miftah, 2018) ingin menawarkan desain keamanan jaringannya tersebut untuk STMIK Eresha untuk mencegah terjadinya hal yang tidak diinginkan dalam jaringan STMIK. (Miftah, 2018) juga menyebutkan pada sistem jaringan komputer di lingkungan STMIK Eresha memiliki kekurangan pada bagian *DHCP Server* dimana *DHCP Server* STMIK tidak memiliki keamanan sama sekali, menyebabkan STMIK Eresha rentan terkena serangan *DHCP* Palsu (*DHCP Rogue*) yang mampu memberikan alamat berupa *gateway* yang salah kepada komputer *client* yang menyebabkan komputer tidak dapat terhubung dengan *server* dan jaringan sekolah.

(Miftah, 2018) menggunakan metode experimental dan simulasi sehingga mampu menyampaikan desainnya dengan jelas. Untuk memberikan hasil desain dan bukti yang valid serta jelas maka dibuat jaringan simulasi dengan menggunakan *Cisco Packet tracer* dan mengkonfigurasi perangkat lainnnya hingga sesuai dengan yang diinginkan. Hasil analisanya ditampilkan dalam bentuk teks dengan hasil yang telah dilakukan dalam simulasi.

Kesimpulan yang didapat bahwa metode *DHCP snooping* mampu memvalidasi *port* yang terpercaya dengan yang tidak terpercaya dan dengan menggunakan sistem keamanan jaringan dengan penerapan keamanan metode *DHCP Snooping*, maka jaringan STMIK lebih aman dibanding sebelumnya dan tidak terganggu oleh *DHCP Server* lain yang berstatus palsu.

Dari jurnal diatas, penulis berpendapat bahwa laporan (Miftah, 2018) memiliki hasil valid yang dapat dipertanggung jawabkan dari hasil analisanya. Namun, cara kerja *DHCP Snooping* dan tata cara konfigurasi tidak dijelaskan secara lengkap, hal ini

menyebabkan ketidakpahaman cara kerja bagi para pembaca. Dengan itu, penulis akan menampilkan landasan teori penulis yang terakhir sebagai perbandingan dan mampu memberikan pembaca alasan kuat kenapa penulis ingin mengangkat topik *DHCP Snooping* sebagai bahan analisis.

Jurnal terakhir berjudul *Study on availability and security of DHCP System in Campus Network*, menurut laporan yang ditulis oleh Chen & Mao pada tahun 2015, *DHCP* digunakan hampir disemua jaringan komputer dengan tujuan untuk memudahkan pembagian IP. Namun, disisi penggunaan yang populer, keamanan jaringan juga perlu ditingkatkan agar IP yang didistribusikan oleh *DHCP Server* merupakan IP yang terdaftar. Masalah keamanan jaringan mulai banyak ditemui dan secara bertahap meningkat dari waktu ke waktu terutama sistem *DHCP* yang dibahas dalam laporan ini. *DHCP Server* palsu atau yang tidak terdaftar akan menyebabkan kesalahan dalam konfigurasi sehingga menyebabkan serangan berupa *DOS (Denial of Service)* pada jaringan. Disisi lain, adapun karyawan yang tidak memiliki izin untuk mengakses bagian tertentu dalam jaringan akan menyamar dengan identitas komputernya yang palsu dan masuk tanpa diketahui oleh pihak yang berwenang. Untuk itu, diperlukan penerapan keamanan jaringan untuk meminimalisir terjadinya hal yang tidak diinginkan.

Metode analisis yang dipakai oleh Chen & Mao ialah dengan membangun jaringan simulasi dan menyusun satu persatu masalah yang akan terjadi pada jaringan komputer, dan melakukan analisa cara kerja, serta cara menanggulanginya.

Hasil kesimpulan yang didapat oleh Chen & Mao berupa beberapa kasus keamanan sistem *DHCP* menghasilkan data yang dapat dijadikan sebuah teori. Hasil analisa setiap masalah dalam laporan ini mampu memberikan solusi yang tepat sesuai dengan akar masalahnya, solusi yang diberikan telah dicoba sesuai dengan masalah keamanan jaringan yang tercantum dalam laporan dan percobaan berhasil untuk jaringan simulasi.

Berdasarkan penelitian yang dilakukan oleh (Ariyadi, 2017), (Miftah, 2018) dan (Chen & Mao, 2015) menghasilkan sebuah kesimpulan dari penulis, bahwa penerapan keamanan jaringan dengan metode *DHCP Snooping* mampu menyaring alamat IP palsu yang tidak terdaftar dalam DHCP server asli sehingga mampu meminimalisir terjadinya serangan yang berpotensi menghambat jalannya jaringan *DHCP Server* seperti contoh *DHCP Rogue*. Dari ketiga jurnal yang telah penulis paparkan, masing-masing memiliki informasi penting yang dapat dipetik dan digabungkan untuk kepentingan laporan penulis. Untuk itu, ketiga jurnal di atas akan penulis jadikan landasan untuk membuktikan teori yang telah dikemukakan oleh ketiga penulis di atas untuk kemudian dijadikan bahan analisis dan menghasilkan laporan karya ilmiah penulis dengan kandungan isi yang lebih lengkap dan jelas.

2.1 Landasan Teori

Analisis keamanan jaringan DHCP Snooping diperkuat dengan sejumlah landasan teori. Landasan teori berupa sekumpulan teori-teori yang digunakan untuk memperkuat teori dalam sebuah penelitian. Teori-teori yang digunakan penulis dalam penelitian dijabarkan sebagai berikut:

2.2.1 OSI Layer

Struktur jaringan bergerak dengan adanya lapisan *Open System Interconnection* atau yang biasa penulis sebut *OSI Layer*. Dalam protokol *OSI Layer* terdapat 7 buah lapisan layanan. Masing-masing lapisan layanan bekerja dengan fungsi yang berbeda-beda, namun terintegrasi satu sama lain, sehingga sebuah jaringan sistem komputer mampu berkomunikasi dan menyebarkan data (Muhammad & Hasan, 2016).

Setiap lapisan dalam *OSI Layer* tersusun atas beberapa lapisan yang diikuti oleh lapisan yang lebih rendah dari berikutnya, lapisan yang lebih rendah ini akan memberikan layanan kepada lapisan yang berada di atasnya. Lapisan *OSI Layer* yang terdiri dari 7 lapisan akan penulis jelaskan sebagai berikut:

1) *Application Layer*
   Lapisan ini merupakan lapisan yang memberikan antarmuka dan layanan aplikasi kepada pemakai akhir (*end user)*. Protokol yang biasanya berjalan pada lapisan ini adalah NFS, SMTP, FTP, dan HTTP.
2) *Presentation Layer*
   Lapisan ini merupakan lapisan yang berfungsi mentranslasikan data karena tiap kode komputer berbeda, maka dari itu, diperlukan peran translasi dalam layer ini, sehingga kode mampu dikenal oleh semua komputer. Protokol yang terdapat dalam layer ini berupa perangkat lunak seperti *redirector software*, layanan *workstation (windows NT), network shell (virtual network computing)*.
3) *Session Layer*
   Layer ini memberikan layanan sinkronisasi berupa pendefinisian koneksi untuk dapat dibuat, dipelihara dan apabila telah sinkron akan dihancurkan.
4) *Transport Layer*
   Lapisan ini memberikan layanan berupa pemecahan data menjadi beberapa bagian data, kemudian memberikan nomor urut dalam tiap pecahan data. Pada saat data telah sampai tujuan, pecahan data akan disusun berdasarkan nomor urut yang telah diberikan sebelumnya. Setelah disusun kembali menjadi sebuah data, lapisan ini akan memberikan tanda bahwa data telah diterima dengan sukses.
5) *Network Layer*
   Lapisan ini merupakan lapisan yang berfungsi untuk menambahkan *header* untuk paket yang dikirim, menambahkan alamat IP dan juga berfungsi menentukan rute yang akan dipakai pada saat pengiriman paket melewati transmisi jaringan.
6) *Data Link Layer*
   Lapisan ini bertugas memberikan *frame* atau dengan kata lain kumpulan bit data yang dikelompokkan menjadi *format* dalam paket yang akan dikirim, caranya dengan penambahan alamat fisik tujuan ke dalam paket.
7) *Physical Layer*
   Lapisan ini bertugas mentranslasikan fisik dari informasi yang diterima dari paket untuk kemudian menjadi sebuah jalur sinyal yang aktual, tanpa memodifikasi apapun dari informasi yang diterima dari dalam paket.

2.2.2 TCP & UDP

Transmission Control Protocol (TCP) merupakan protokol yang bertugas mengatur komunikasi 2 arah antar komputer. Komputer yang terhubung satu sama lain melalui internet akan berkomunikasi satu sama lain menggunakan protokol TCP (Sari, Sudarsono, & Hayadi, 2013).

TCP bekerja dengan basis *connection-oriented*, menurut penelitian dari Latipa Sari, dkk pada tahun 2013. *Connection-oriented* dengan maksud komputer yang ingin melakukan pertukaran data butuh membuat sebuah hubungan untuk mengonfirmasi bahwa komputer-komputer yang ingin melakukan pertukaran data dalam keadaan siap menerima data dari pengirim, disisi lain, pengirim juga harus siap mengirim data ke penerima. Sebelum pengiriman data, TCP bertugas mengecek apakah jalur data yang ingin dikirim aman, apabila tidak, TCP akan memberikan sinyal berupa pesan *error,* apabila aman, pertukaran data akan dilanjutkan. Paket data yang terlalu besar juga akan dipecah menjadi beberapa bagian untuk mempermudah pengiriman data. Pada proses ini, IP berperan sebagai kurir yang berfungsi merutekan jalur terbaik untuk pengiriman data. IP akan mengirim sampai ke tujuan, namun IP tidak bertanggung jawab apabila ada pecahan paket yang hilang dikarenakan IP mengirim tanpa mengetahui urutan data. IP hanya berperan sebagai kurir yang mengirim tanpa tahu isi paket yang dikirim.

Apabila paket telah sampai tujuan, TCP akan mengkonfirmasi bahwa data telah sampai pada tujuan, kemudian akan memutuskan hubungan komunikasi tersebut.

Berbeda dengan TCP, protokol UDP atau dengan nama lain *User Datagram Protocol* tidak memerlukan hubungan apapun karena jenis protokol ini lebih mengutamakan kecepatan transmisi data. Biasanya UDP digunakan untuk fasilitas yang *real-time* seperti *streaming* video dan *game online* berbasis *client server.* Maka dari itu, UDP tidak perlu mengadakan hubungan tertentu dengan tujuan dan langsung mengirim data tanpa mengkonfirmasi penerima sudah siap atau belum. Karena apabila mementingkan adanya hubungan konfirmasi (*session*) akan menambah *delay* pengiriman data dari satu ke yang lain. UDP sering disebut protokol *connectionless* yang artinya tanpa aktifitas *handshaking* / tanpa konfirmasi pengirim dengan status penerima sudah siap atau belum, seperti yang dilakukan oleh TCP. Hal ini merupakan kelemahan dari protokol UDP yang berisiko hilangnya data yang dikirim, apabila penerima belum siap menerima data yang dikirim (Rizkilla, M, & Mulyana, 2016).

2.2.3 Classless IP

Classless IP merupakan golongan IP tanpa kelas atau dengan pengertian lain yaitu pengalamatan IP yang tidak mengenal adanya kelas, biasanya menggunakan metode CIDR yang berkepanjangan Classless-Inter Domain Routing. Ciri-ciri dari classless IP ini ialah pengalamatan yang didahului tanda (/) slash pada bagian belakang sebuah alamat IP. Contoh : 192.168.1.1/24 (bagian sebelum slash merupakan alamat IP dan setelah slash merupakan classless IP). Pengalamatan IP/host dengan menggunakan subnet mask yang berbeda dengan metode routing protocol seperti RIPv2, EIGRP, OSPF dimana mampu memberikan informasi subnet sehingga dapat menghemat jumlah IP/host (Bohdanowicz & Henke, 2014).

2.2.4 VLAN

VLAN atau dengan nama lain *Virtual Local Area Network* merupakan sebuah jenis jaringan yang tidak dibatasi oleh lokasi fisik semisal LAN. Maka dari itu, menyebabkan jaringan *VLAN* mampu dikonfigurasi secara virtual tanpa menuntut lokasi fisik perangkat keras. Agar *VLAN* bisa digunakan, diperlukan switch yang bisa dikonfigurasi dan memastikan seluruh switch yang berada dalam satu jaringan memiliki konfigurasi yang sama. *VLAN* secara fisik memang terlihat seperti satu jaringan, namun secara logika, *VLAN* merupakan jaringan yang berbeda. Dengan adanya *VLAN* maka kemungkinan seluruh jaringan terganggu akan sangat rendah karena *VLAN* membagi satu jaringan menjadi beberapa jaringan secara logika, sehingga apabila satu vlan terganggu tidak akan terpengaruh *VLAN* yang lain (Putra & Wiwin Sulistyo, S.T., 2014).

2.2.5 Cisco Packet Tracer

Packet tracer merupakan aplikasi lunak yang berfungsi sebagai mesin virtualisasi atau simulasi untuk proses pembangunan jaringan virtual. Di dalam aplikasi ini juga disediakan berbagai perangkat keras virtual untuk memudahkan pengguna untuk menggunakannya secara virtual tanpa harus membeli perangkat keras yang sebenarnya. Perangkat keras virtual yang disediakan dalam aplikasi terbatas hanya pada perangkat *cisco*. Dengan aplikasi simulasi ini, para pengguna dapat belajar cara konfigurasi setiap perangkat *cisco* dalam jaringan dengan mudah dan pengoperasian *user interface* yang ramah (Javid, 2014). *Cisco packet tracer* mampu mengecek lalu lintas paket dalam jaringan simulasi yang dibuat di dalamnya, sehingga pengguna dapat menganalisis jalannya jaringan simulasi yang ingin dibuat dan mengetahui kelebihan dan kelemahan dari simulasi jaringan yang telah didesain pengguna.

Cisco packet tracer dikembangkan oleh *Cisco System Inc.* dan banyak digunakan oleh mahasiswa yang mengikuti program kursus *CCNA* dan *CCNP*. *Packet tracer* mampu mensimulasikan jaringan komputer yang realistis sehingga masalah yang akan terjadi pada desain jaringan tersebut dapat dianalisa tanpa harus menggunakan jaringan yang sebenarnya (Kocaleva, Stojanovik, & Zdravev, 2015). Pengoperasian *Packet tracer* secara *GUI (Graphical User Interface)* namun ada juga

bagian dimana konfigurasi perangkat keras seperti *router* dan *switch* menggunakan *CLI (Command Line Interface).*

2.2.6 DHCP Server

Dynamic Host Control Protocol atau yang biasa disingkat dengan *DHCP* merupakan protokol Internet dimana bertugas mendistribusikan segala informasi *TCP/IP* secara langsung kepada komputer yang terhubung dan menggunakan protocol *TCP/IP*. Protokol *DHCP* merupakan hasil perkembangan protokol jaringan *BOOTP* atau yang dikenal dengan *Bootstrap Protocol* yang memiliki kelebihan berupa alokasi otomatis ke berbagai alamat jaringan yang terhubung satu sama lain (Husni, 2014).

DHCP memiliki 2 fungsi utama. Yang pertama *DHCP* berfungsi sebagai *persistent storage* atau dengan arti lain media penyimpanan menetap dari jaringan parameter untuk *client. DHCP* menyimpan sebuah *key-value* dari setiap *client* karena *key-value* ini merupakan tanda pengenal yang unik dalam tiap komputer *client* dan mengandung parameter konfigurasi *client*. Tanda pengenal unik yang terdapat dalam masing-masing komputer *client* merupakan nomor subnet IP.

Fungsi *DHCP* yang kedua sebagai pengalokasi IP atau alamat jaringan *client* baik secara temporer maupun secara permanen. Pengalokasi dengan maksud bahwa mekanisme *DHCP* tidak akan melakukan realokasi kepada alamat yang telah diberikan kepada *client* sebelumnya dan mencegah terjadinya pengiriman alamat yang sama setiap kali *client* meminta alamat kepada *DHCP Server*. Maka dari itu, *DHCP* tidak akan mengirimkan alamat IP yang sama kepada *client* untuk lebih dari satu *node* (jumlah perangkat dalam jaringan) pada saat yang sama, peraturan ini tetap berlaku walaupun *node* direstart berkali-kali (Husni, 2014).

DHCP memiliki beberapa fakta dalam pengalamatan sebuah alamat IP, sebagai berikut:

1) DHCP menggunakan port UDP 67 untuk server dan port UDP 68 untuk client. Penjelasan yang lebih detail akan dijelaskan pada subbab "2.2.7 cara kerja DHCP server".
2) DHCP menggunakan TCP/IP agar dapat berkomunikasi ke dalam jaringan.
3) DHCP merupakan protokol layer 7 dalam OSI Layer.
4) Protokol yang digunakan DHCP (TCP dan UDP) merupakan transport protokol layer 4 pada OSI Layer.

2.2.7 Cara kerja DHCP Server

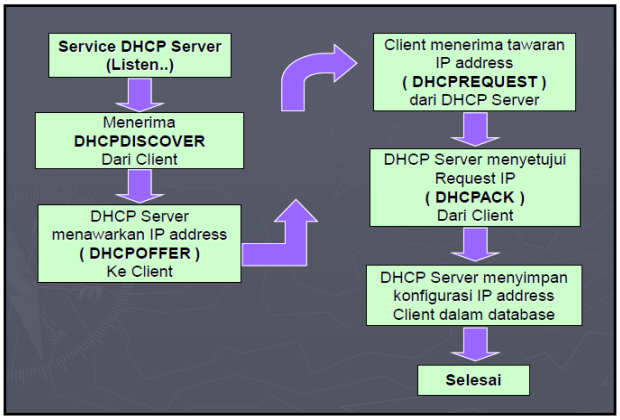
Cara kerja *DHCP Server* dimulai dari sisi *client* yang mengirimkan perintah *broadcast* yang biasanya disebut dengan *DHCP Discover* yang didalam pesan ini terkandung *MAC address client* ke jaringan untuk mencari keberadaan *DHCP Server*. Pada saat ini, sisi *client* menggunakan *port UDP* 68 dan mencari tujuan server yang menggunakan *port UDP* 67.

Ketika *DHCP Server* mendapat sinyal pesan *DHCP Discover* dari *client*, server mulai menentukan alamat untuk diberikan kepada *client* sesuai dengan konfigurasi yang telah diatur dalam server sebelumnya. Server kemudian mengalokasikan alamat yang tepat untuk dibagikan kepada *client* dan mengirim balik alamat yang telah ditentukan oleh server dengan nama *DHCP Offer* kepada *client.* Pada saat ini, sisi server yang menggunakan *port UDP* 67 akan mengirim pesan ke *port UDP* 68 yang digunakan *client*. Di dalam pesan *DHCP Offer* terdapat informasi *IP Address* serta protokol *TCP/IP* lain agar *client* mampu menggunakannya untuk berkomunikasi dengan jaringan.

Untuk menerima pesan dari server, *client* akan mengirimkan pesan berupa *DHCP Request* untuk mengkonfirmasi kepada server bahwa *client* benar bermaksud untuk memakai alamat tersebut. Pada saat ini, sisi *client* menggunakan *port UDP* 68 dan menjawab server yang menggunakan *port UDP* 67.

Kemudian server mengirimkan *DHCP Pack* (*packet acknowledgement*) kepada *client* dan server akan memperbaharui informasi *database* dalam server dimana IP tertentu telah dipinjamkan kepada *client* (Husni, 2014). Tahap terakhir berupa *DHCP Inform* dari *client* yang menginformasikan kepada server bahwa sisi *client* telah menerima IP secara *broadcast* yang diberikan oleh server. Untuk memperjelas

penjelasan dan ilustrasi pada paragraf diatas, disajikan *Gambar 1* dibawah sebagai berikut:



Gambar 1: *Diagram Alur pertukaran pesan antara Client dan Server*

2.2.8 Keamanan Jaringan

Pengertian dari keamanan jaringan merupakan sebuah proses mencegah serta mengidentifikasi pihak pengguna computer yang tidak semestinya ada dalam jaringan computer (penyusup) yang memiliki tujuan merugikan jaringan computer yang disusupi.

Sebuah system keamanan jaringan berfungsi untuk mengantisipasi adanya ancaman terhadap jaringan computer tersebut baik dalam bentuk fisik (merusak bagian computer secara fisik) maupun secara logika (pencurian akun atau data penting orang lain).

Prinsip dan layanan perlindungan keamanan terbagi menjadi beberapa hal sebagai berikut (Rumalutur, 2014):

1) Kerahasiaaan (*Confidentiality*)
   pencegahan pihak yang tidak memiliki wewenang untuk tidak melihat informasi yang sensitif atau bersifat rahasia.
2) Integritas (*integrity*)
   Penjaminan data yang ada tidak berubah dan konsisten sesuai dengan bentuk apa adanya tanpa mengalami perubahan.
3) Otentikasi (*Authentication*)
   pemastian suatu layanan yang meyakinkan identitas pengguna komunikasi berada dalam jaringan yang aman dan benar.
4) Tidak terjadi penyangkalan (*Non-repudiation*)
   pencegahan baik pihak penerima maupun pihak pengirim mengalami penyangkalan pesan yang dikirim/diterima.
5) Ketersediaan (*Avaiability*)
   penjaminan system yang tersedia agar dapat selalu digunakan setiap kali ada permintaan dari pengguna
6) Akses kendali (*Access Control*)
   pembatasan dan pengontrolan akses pengguna.

2.2.9 DHCP Snooping

DHCP snooping merupakan sebuah metode yang diterapkan dalam jaringan komputer untuk peningkatan keamanan jaringan komputer yang menggunakan *DHCP server. DHCP snooping* dapat dilakukan melalaui konfigurasi switch dalam jaringan *LAN (Local Area Network)* dengan mengizinkan client jaringan komputer menerima sumber IP dan alamat jaringan komputer dari *DHCP server* melalui *port switch* yang terpercaya untuk terhubung ke jaringan komputer. Teknik *DHCP snooping* menyimpan informasi tentang alamat IP di dalam *database* switch LAN. Selain dari itu, *DHCP Snooping* merupakan komponen utama dalam keamanan akses jaringan LAN karena juga dapat digunakan sebagai fitur keamanan lain berupa penjaga ARP dinamis dan sumber IP (Ariyadi, 2017).

2.2.10 Cara Kerja DHCP Snooping

DHCP Snooping bekerja seperti sebuah *firewall* dimana fungsi dan tugas utamanya untuk membedakan mana sumber IP yang terpercaya dan sumber yang tidak dapat dipercaya (Khan, Alshomrani, & Qamar, 2013). Metode ini bekerja membedakan mana sumber terpercaya dengan tidak dari database yang telah disimpan dan dikonfigurasi sebelumnya, yang menyimpan alamat sumber IP terpercaya dan menolak sumber selain dari itu. Biasanya, *DHCP Snooping* dalam penggunaannya dalam jaringan komputer perusahaan, *switch* yang berada dalam kontrol *admin* perusahaan merupakan sumber terpercaya, termasuk *router* dan *server* yang terhubung dan terdaftar dalam jaringan peruahaan. *Port switch* yang kosong (tidak digunakan sama sekali) biasanya akan secara otomatis terdaftar sebagai sumber yang tidak dapat dipercaya (Cisco, 2016).

2.2.11 Jenis ancaman keamanan DHCP Server

Terdapat beberapa jenis ancaman terhadap jaringan *DHCP Server* sehingga pihak yang tidak bertanggung jawab mampu merusak jairngan komputer perusahaan. Beberapa ancaman yang harus diperhatikan antara lain sebagai berikut:

1) *DHCP Rogue*

   Pemalsuan *DHCP server* palsu atau yang biasa disebut dengan *DHCP Rogue*, yang cara kerjanya dengan pembuatan sebuah server *DHCP* yang palsu dan dihubungkan dalam jaringan target, menyebabkan client dalam jaringan tersebut mendapatkan IP yang didistribusikan dari *DHCP Server* palsu tersebut (Kadafi & Kusnawi, 2015).

2) *IP/MAC Spoofing*

   Jenis serangan ini menggunakan *IP, Mac* atau kombinasi keduanya yang berstatus palsu dan mengirimkannya paket ke target jaringan agar bisa mengakses jaringan dan mendapatkan hak akses sesuai dengan posisi alamat *IP, Mac* yang terdaftar dalam jaringan (Szeto, Jain, Suresh, & Kwan, 2013).

3) *DHCP Flooding*

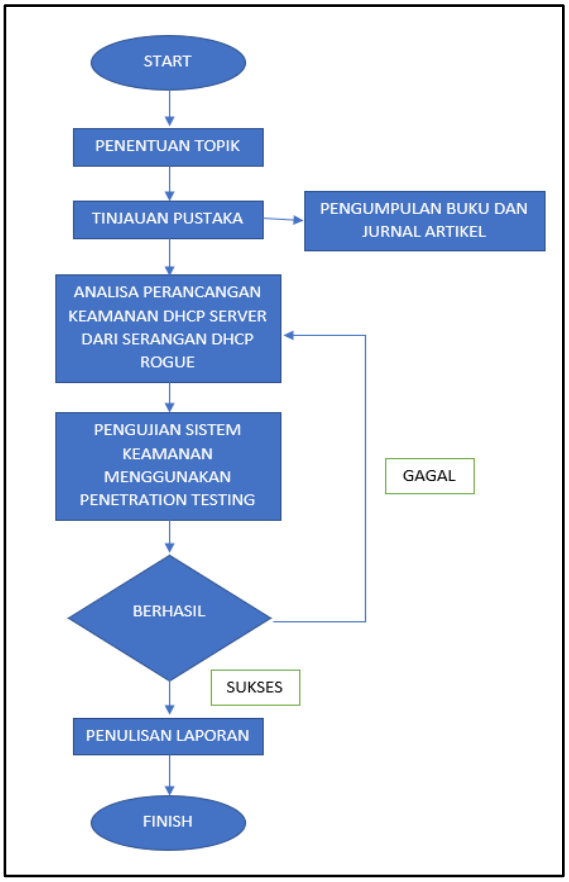
   DHCP Flooding memiliki cara kerja dengan mengirimkan permintaan dalam jumlah banyak ke *DHCP Server* oleh peretas. *DHCP Server* akan otomatis membagikan sejumlah IP yang diminta dan pada batasan tertentu akan menghabiskan alamat IP dalam *DHCP Server.* Hal ini mengakibatkan *client* yang ingin meminta alamat IP kepada *DHCP server* tidak mendapatkan IP karena alamat IP pada *DHCP Server* telah habis diminta peretas. Sehingga *client* dalam jaringan tidak dapat terhubung ke dalam jaringan (Wu, Li, Chen, & An, 2016).

Dari beberapa ancaman *DHCP server* diatas, penulis hanya akan menganalisis mengenai *DHCP Rogue*, alasan penulis ingin menganalisis lebih dalam mengenai *DHCP Rogue* dikarenakan metodenya yang sederhana menyebabkan banyak oknum yang tidak bertanggung jawab memiliki keinginan untuk mencobanya. Metode penyerangan yang sederhana ini mampu menyebabkan kekacauan dalam jaringan perusahaan yang mampu menyebabkan kerugian bagi perusahaan hanya karena adanya oknum nakal yang ingin mencobanya. Selain faktor kesengajaan, dapat juga terjadi ketidaksengajaan karena kesalahan dalam konfigurasi jaringan yang menyebabkan malfungsi dalam jaringan. Karena faktor-faktor yang disebutkan tadi, penulis ingin menganalisa cara kerjanya dan memberikan sebuah solusi agar pengguna jaringan dapat terhindar dari ancaman tersebut.

3. Metode Penelitian

3.1 Alur Penelitian

Alur penelitian merupakan rangkaian langkah-langkah yang dilakukan dalam perancangan karya ilmiah penulis, agar rancangan berjalan teratur dan sesuai dengan yang direncanakan. Maka penulis membuat rancangan alur peneltian dengan urutan sebagai berikut:



Gambar 2 : Flowchart alur penelitian

Dari beberapa tahapan dalam flowchart pada Gambar 2, akan dijelaskan secara deskriptif setiap tahapan yang penulis terapkan sebagai berikut:

1) Penentuan topik merupakan tahapan awal dalam perancangan karya ilimiah dimana penulis memikirkan sebuah topik yang akan dibahas rinci dalam karya ilimiah yang akan ditulis.
2) Tahap pengumpulan data & informasi merupakan tahap terpenting, karena landasan teori yang baik mendukung penulisan karya ilmiah untuk berjalan dengan baik dan optimal. Teori yang telah dikemukakan sebelumnya dapat digunakan kembali dan dilengkapi dengan informasi terbaru sehingga laporan yang ditulis oleh penulis mampu mengikuti perkembangan teknologi.
3) Tahapan analisa untuk menganalisis apa yang menjadi masalah pembahasan topik ini, sehingga mampu menyusun beberapa rumusan masalah dan menjadi pembahasan utama laporan karya ilmiah.
4) Tahap pengujian dengan menggunakan metode penetration testing sebagai metode utama untuk membuktikan argumen bahwa *DHCP Snooping* mampu menangkal serangan *DHCP Rogue.*
5) Apabila langkah diatas berhasil maka dilanjutkan dengan penulisan laporan karya ilmiah sebagai dokumentasi hasil penelitian, dan apabila tidak berhasil, maka penulis mengulangi langkah analisa perancangan untuk menyusun kembali bahasan utama penelitian untuk kemudian dilakukan tahap pengujian ulang.
6) Tahap penulisan laporan sebagai dokumentasi formal untuk disajikan sebagai tahap akhir penelitian.

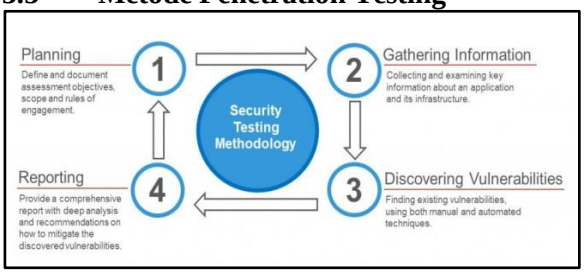
3.2 Analisa Permasalahan

Karya ilmiah yang dibuat penulis dengan metode penelitian simulasi bertujuan untuk membuktikan apakah *DHCP Snooping* mampu mengoptimalkan keamanan jaringan dengan menggunakan jaringan simulasi. Penulis fokus akan membahas *DHCP snooping* untuk menangkal *DHCP rogue* sebagai ancaman keamanan jaringan, karena *DHCP Rogue* mampu mencuri data penting perusahaan dengan menggunakan *sniffing* pada *wireshark* apabila *DHCP server* peretas berhasil dipenetrasi ke jaringan perusahaan (penulis menjelaskan cara kerjanya dalam bab 4). Namun dari sisi bahayanya, ancaman tersebut dapat ditangkal dengan mudah hanya dengan menggunakan *DHCP snooping*. Untuk membuktikannya, penulis membuat sebuah skenario jaringan perusahaan. Jaringan perusahaan terdiri dari 3 *switch*, 10 *client*, 2 *router* dimana semuanya terhubung dengan ISP. *Router* terbagi menjadi *router trusted* yang berasal dari jaringan perusahaan sendiri dan *router untrusted* yang merupakan *router* peretas yang berusaha untuk masuk dan mengambil kendali *client* perusahaan.

Disediakan *router trusted* dan *untrusted* dengan settingan *DHCP server* dimasing-masing

router dan terhubung satu sama lain melalui *switch* untuk membuktikan bahwa dengan adanya *DHCP server* tanpa menggunakan *DHCP snooping* menyebabkan *client* tidak konsisten mendapatkan IP dari sumber terpercaya (*Router trusted* jaringan perusahaan) sehingga beberapa *client* akan mendapatkan IP dari *router untrusted* peretas. Penyerangan *DHCP Rogue* dapat dilanjutkan apabila jaringan perusahaan terkoneksi satu jaringan dengan peretas. Karena fungsi *DHCP Snooping* menghambat *DHCP Server* palsu untuk masuk ke jaringan perusahaan, mengakibatkan peretas tidak mampu melakukan *sniffing packet* karena tidak dalam satu jaringan, dan alhasil tidak mampu melakukan pencurian data penting perusahaan.

3.3 Metode Penetration Testing



Gambar 3 : Tahap Penetration Testing

(*Lihat Gambar 3*) Tahap *penetration testing* sebagai metode penelitian yang digunakan oleh penulis. *Penetration testing* dibagi menjadi 5 tahap secara umum, yaitu

1) *Planning* yang merupakan tahap analisa apa saja yang dibutuhkan untuk melakukan metode penelitian *penetration testing*. Dalam topik penulis, tahap *planning* merupakan tahap pengumpulan data-data informasi jaringan yang dibutuhkan, bagaimana cara jalannya jaringan simulasi dan definisi target.
2) Kemudian tahap *Information gathering* yang merupakan tahap pengumpulan informasi yang dibutuhkan untuk melakukan eksploitasi dalam jaringan simulasi, dalam penelitian penulis, tahap ini akan mengumpulkan data jaringan seperti *IP*, *Gateway*. Kemudian definisi alur penyerangan, dan data apa saja yang akan diambil.
3) kemudian tahap *vulnerability assessment* merupakan tahap dimana penulis menganalisa celah keamanan dalam jaringan simulasi dan menjadikan celah tersebut sebagai bahan analisa, karena secara umum tahap ini merupakan tahap analisis celah keamanan apakah bias diserang secara manual atau secara otomatis dengan menggunakan perangkat lunak.
4) Kemudian dilanjutkan ke tahap *exploiting*, dimana penulis berperan seolah-olah sebagai pencuri data untuk mensimulasikan apa yang akan terjadi pada celah keamanan tersebut. Tahap *exploiting* secara umum merupakan tahap penetrasi menuju jaringan target untuk kebutuhan percobaan sehingga mampu mendefinisikan kelebihan serta kelemahan dari jaringan tersebut.
5) Dan tahap terakhir ialah *reporting*, yaitu tahap pelaporan hasil analisa tahap yang telah dilakukan penulis.

3.4 Kebutuhan Sistem

Untuk merancang dan menerapkan skenario ke dalam sebuah simulasi dibutuhkan perangkat keras dan perangkat lunak yang memadai. Untuk itu, penulis akan menguraikan spesifikasi perangkat keras dan perangkat lunak yang dipakai selama perancangan skenario dan simulasi sebagai berikut:

1) Perangkat keras (*Hardware*)

   Satu unit laptop yang digunakan untuk mendesain skenario dan simulasi jaringan dalam perangkat lunak dengan spesifikasi sebagai berikut:

- Processor Intel ® Core ™ i5-4200 CPU 1.60 GHz
- Memory (RAM) 8 GB
- Harddisk 500 GB

2) Perangkat lunak (*Software*)

   Cisco Packet Tracer sebagai perangkat lunak mampu menyediakan berbagai kebutuhan perangkat keras dalam bentuk virtual diaplikasinya sehingga memudahkan perancangan jaringan

No	Komponen Hardware	IP Address
1	Trusted Router (DHCP Server)	Network 11.11.11.0/24
2	Untrusted Router (DHCP Server)	Network 192.168.2.0/24
3	Switch 1 (PC Switch)	-
4	Switch 2 (Core Switch)	-
5	Switch 3 (Laptop Switch)	-
6	PC 1 (Client)	Tergantung Pembagian DHCP Server
7	PC 2 (Client)	Tergantung Pembagian DHCP Server
8	PC 3 (Client)	Tergantung Pembagian DHCP Server
9	PC 4 (Client)	Tergantung Pembagian DHCP Server
10	PC 5 (Client)	Tergantung Pembagian DHCP Server
11	PC 6 (Client)	Tergantung Pembagian DHCP Server
12	PC 7 (Client)	Tergantung Pembagian DHCP Server
13	PC 8 (Client)	Tergantung Pembagian DHCP Server
14	PC 9 (Client)	Tergantung Pembagian DHCP Server
15	PC 10 (Client)	Tergantung Pembagian DHCP Server

simulasi dan skenario permasalahan tanpa harus menggunakan perangkat keras yang nyata.

Penulis menyiapkan sebuah skenario yang ingin penulis buat dalam aplikasi *Cisco Packet Tracer* dengan menggunakan hardware virtual (*Lihat Tabel 1*)

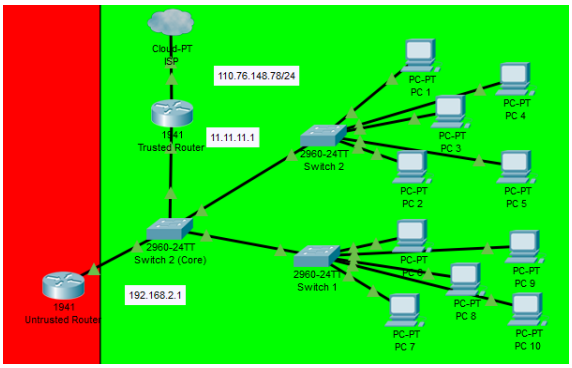
Tabel 1

komponen hardware simulasi

4. Implementasi

4.1 Implementasi dan Tahap Konfigurasi

Langkah implementasi yang akan dilakukan penulis membutuhkan beberapa konfigurasi dan komponen virtual yang diperlukan seperti yang telah disebutkan pada bab 3, sehingga apabila digabungkan dan perancangan scenario simulasi akan terliaht seperti Gambar 4 dibawah sebagai berikut:



Gambar 4 : Susunan Jaringan Simulasi

Pada bagian dengan arsiran hijau menandakan jaringan utama perusahaan dan bagian dengan arsiran merah menandakan pihak yang ingin mencemari jaringan perusahaan.

4.1.1 Pengadaan hardware virtual dalam simulasi

Untuk membangun sebuah jaringan simulasi, diperlukan beberapa perangkat keras

vitual yang telah disediakan dalam perangkat lunak *Cisco Packet Tracer*. Perangkat yang diperlukan dalam jaringan disebutkan dalam Tabel 2 sebagai berikut:

Tabel 2

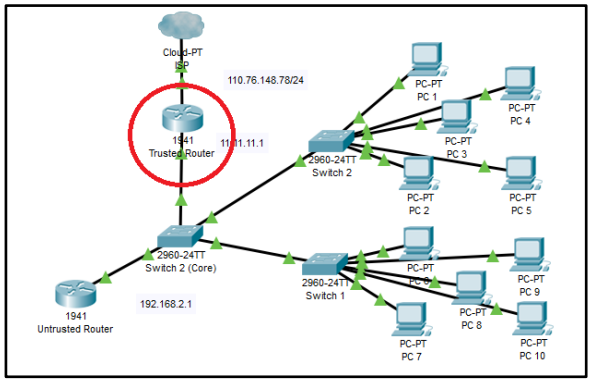
Perangkat yang dibutuhkan dalam jaringan simulasi

No	Nama Perangkat	Jumlah
2	Switch	3 Buah
3	Router	2 Buah
4	PC	10 Buah

4.1.2 Konfigurasi DHCP Server pada Trusted dan Untrusted Router

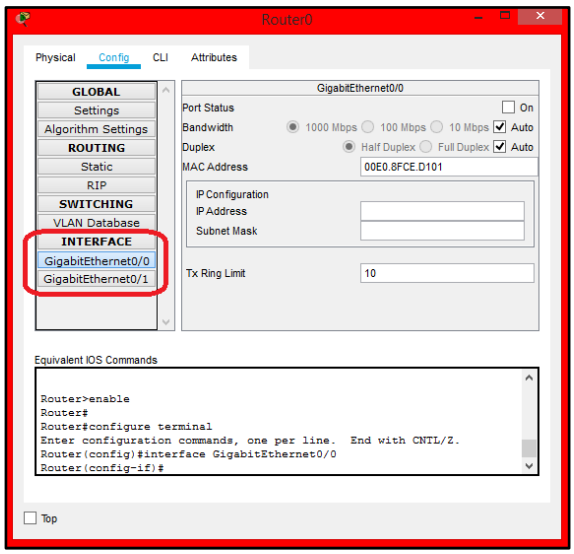
Pada tahapan ini, penulis mengkonfigurasi router *trusted* dan *untrusted*, tahapan ini mengkonfigurasi 2 router yang memiliki cara kerja yang sama, yaitu sebagai *DHCP server* yang berfungsi membagikan *range* IP yang telah dikonfigurasi sebelumnya. Namun, hanya salah satu router yang diakui dalam simulasi ini yaitu router *trusted* dengan alamat IP 11.11.11.0/24. Sedangkan router *untrusted* dengan alamat IP 192.168.2.0/24 akan berperan sebagai peretas jaringan dengan menyebarkan *range* IP yang tidak diakui oleh jaringan sebenarnya. Tujuannya untuk membuktikan pengaruh *DHCP snooping* bagi keamanan jaringan perusahaan dengan membandingkan antara jaringan yang tidak memiliki konfigurasi *DHCP snooping* dengan jaringan yang menggunakan konfigurasi *DHCP snooping*. Kedua router ini akan terhubung ke ISP jaringan simulasi. Langkah konfigurasi router *trusted* dan *untrusted* akan dijelaskan satu persatu sebagai berikut:

1) Langkah pertama penulis akan mengkonfigurasi router *trusted* yang diakui dan dimiliki oleh jaringan perusahaan simulasi. *Router trusted* berada diposisi seperti yang ditunjukkan Gambar 5.



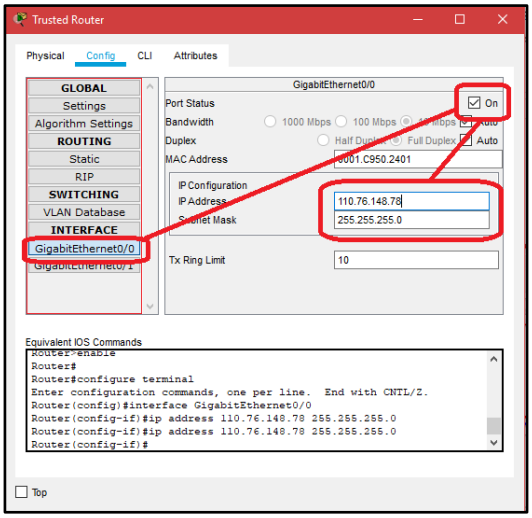
Gambar 5 : Posisi Trusted Router dalam jaringan simulasi

2) Klik gambar router *trusted*, kemudian pilih tab *config* maka akan muncul jendela seperti pada Gambar 6 di bawah:



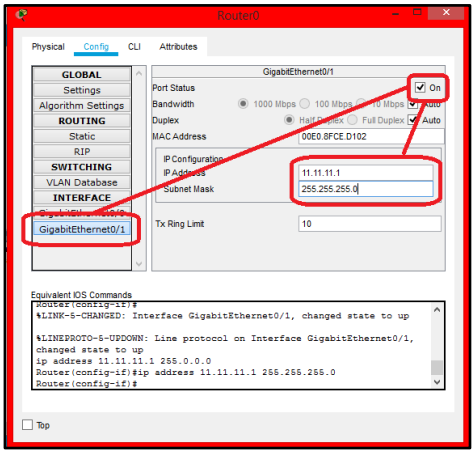
Gambar 6 : Jendela Config Trusted Router

3) Pada tahapan ini, penulis akan mengkonfigurasi *gateway* router. Karena router terhubung dengan switch dan server, maka perlu dikonfigurasi 2 *gateway* router. Tekan tombol "GigabitEthernet0/0" untuk mengkonfigurasi port Gig0/0 yang terhubung dengan ISP. Centang bagian "ON" untuk mengaktifkan port dan isi keterangan IP *Address* dengan 110.76.148.78 dengan *subnet* 255.255.255.0, untuk lebih jelasnya silahkan lihat Gambar 7.



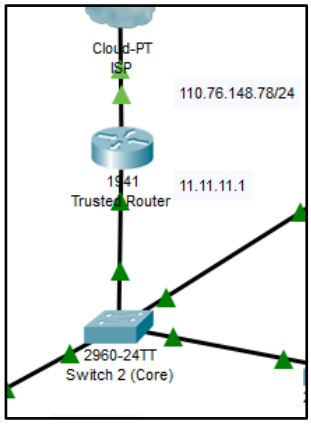
Gambar 7 : Config Port Trusted Router

4) Lakukan hal yang sama sesuai dengan langkah di atas, namun memilih tombol "GigabitEthernet0/1" untuk mengkonfigurasi port Gig0/1 yang mengarah ke switch. Isi keterangan IP *Address* dengan 11.11.11.1 dengan *subnet* 255.255.255.0, untuk lebih jelas silahkan melihat Gambar 8.



Gambar 8 : Config Port Trusted Router

5) Sehingga apabila telah terkonfigurasi dengan benar, akan tampak seperti Gambar 9 di bawah sebagai berikut:



Gambar 9 : Hasil konfigurasi gateway router

6) Langkah selanjutnya penulis akan mengkonfigurasi *DHCP server* dalam *router trusted*. Seperti yang telah ditentukan sebelumnya pada bab 3, *range* IP DHCP *trusted* dalam network 11.11.11.0/24. Berikut konfigurasi lengkapnya terangkum dalam Gambar 10:

```
1 = Router>enable
2 = Router#conf t
3 = Router(config)#service dhcp
4 = Router(config)#ip dhcp pool trusted
5 = Router(dhcp-config)#network 11.11.11.0 255.255.255.0
6 = Router(dhcp-config)#default-router 11.11.11.1
7 = Router(dhcp-config)#dns-server 8.8.8.8
8 = Router(dhcp-config)#exit
```

Gambar 10 : rangkuman langkah config DHCP server

7) (*Lihat Gambar 10*) Pada nomor 1 & 2 merupakan langkah untuk masuk ke *global config mode* agar memiliki hak untuk setting router. Kemudian nomor 3 untuk mengaktifkan perintah konfigurasi *DHCP server* dan langsung memfokuskan input *command* sepenuhnya untuk *DHCP server*. Nomor 4 untuk pemberian nama pada *DHCP server pool*, penulis memberikan nama "*trusted*" yang terdapat pada akhir perintah. Nomor 5 untuk memasukkan *range* IP jaringan yang ingin didaftar dalam *DHCP server*, untuk penelitian ini, penulis menggunakan alamat 11.11.11.0/24. Nomor 6 untuk penentuan *gateway default* yang akan dilalui *client*

pada saat *request* & *accept* IP. Nomor 7 untuk menentukan *DNS server* yang telah penulis buat sebelumnya.

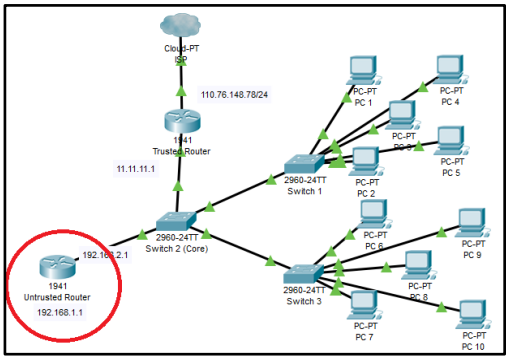
8) Setelah *DHCP Server* selesai, dilanjutkan dengan konfigurasi ISP pada *router trusted.* Konfigurasi yang dilakukan penulis sebagai berikut:

```
1 = Router(config)#ip route 0.0.0.0 0.0.0.0 110.76.148.77
2 = Router(config)#ip name-server 8.8.8.8
3 = Router(config)#access-list 1 permit 11.11.11.0 0.0.0.255
4 = Router(config)#ip nat inside source list 1 interface g0/0 overload
5 = Router(config)#interface g0/0
6 = Router(config-if)#ip nat outside
7 = Router(config-if)#interface g0/1
8 = Router(config-if)#ip nat inside
```

Gambar 11 : Konfigurasi ISP pada router

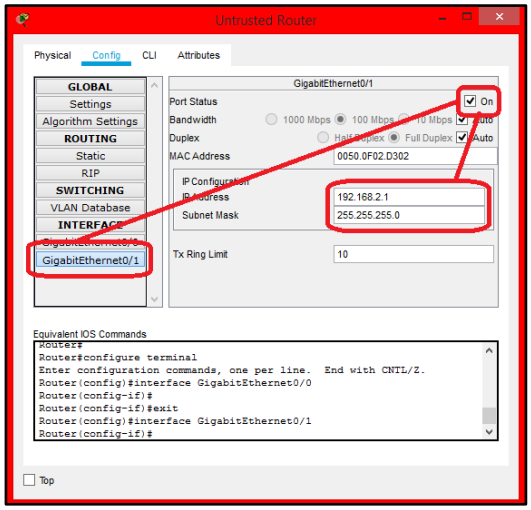
9) (*Lihat Gambar 11*) pada nomor 1 merupakan langkah untuk mengkonfigurasi default gateway menuju ISP. Kemudian pada nomor 2 merupakan langkah untuk mengkonfigurasi DNS Resolver sehingga router mampu terkoneksi ke hostname. Nomor 3 sampai denngan nomor 8 mengkonfigurasi NAT (Network Address Translation) untuk melakukan translasi IP dari ISP menuju jaringan 11.11.11.0/24.

10) Konfigurasi untuk router *trusted* telah selesai. Penulis akan melanjutkan konfigurasi *router untrusted*. Langkahnya sama persis seperti konfigurasi *trusted* router namun dengan input IP yang berbeda. Posisi router *untrusted* berada pada bagian tepat di samping *core* switch seperti yang ditunjukkan Gambar 12 sebagai berikut:



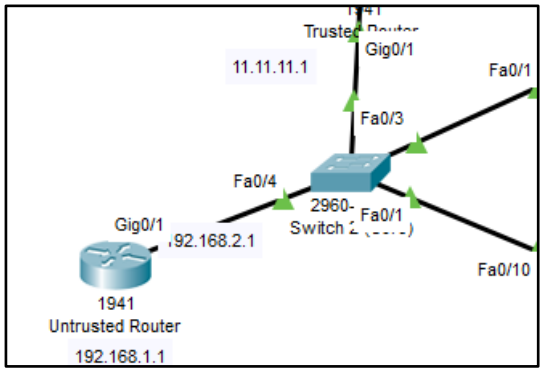
Gambar 12 : Posisi Untrusted Router

11) Tekan bagian router kemudian ke tombol "GigabitEthernet0/1", pastikan centang "ON" untuk mengaktifkan port dan isi keterangan IP *address* denga 192.168.2.1 untuk port Gig0/1 dengan subnet 255.255.255.0 (*Lihat Gambar 13*).



Gambar 13 : Tampilan config port ga0/1

12) Apabila telah selesai dengan konfigurasi tersebut, tampilan akhir akan terlihat seperti Gambar 14.



Gambar 14 : Tampilan akhir Untrusted Router

13) Langkah selanjutnya penulis akan mengkonfigurasi *DHCP server* dalam *router untrusted*. Seperti yang telah ditentukan sebelumnya pada bab 3, *range* IP DHCP *untrusted* dalam network 192.168.2.0/24. Berikut konfigurasi lengkapnya terangkum dalam Gambar 15:

```
1 = Router>enable
2 = Router#conf t
3 = Router(config)#service dhcp
4 = Router(config)#ip dhcp pool untrusted
5 = Router(dhcp-config)#network 192.168.2.0 255.255.255.0
6 = Router(dhcp-config)#default-router 192.168.2.1
7 = Router(dhcp-config)#dns-server 8.8.8.8
8 = Router(dhcp-config)#exit
```

Gambar 15 : rangkuman langkah config DHCP server

14) (Lihat Gambar 15) Pada nomor 1 & 2 merupakan langkah untuk masuk ke *global config mode* agar memiliki hak untuk setting router. Kemudian nomor 3 untuk mengaktifkan perintah konfigurasi *DHCP server* dan langsung memfokuskan input *command* sepenuhnya untuk *DHCP server*. Nomor 4 untuk pemberian nama pada *DHCP server pool,* penulis memberikan nama "*untrusted*" yang terdapat pada akhir perintah. Nomor 5 untuk memasukkan *range* IP jaringan yang ingin didaftar dalam *DHCP server*, untuk penelitian ini, penulis menggunakan alamat 192.168.2.0/24. Nomor 6 untuk penentuan *gateway default* yang akan dilalui *client* pada saat *request* & *accept* IP. Nomor 7 untuk menentukan *DNS server*. Karena ini merupakan *untrusted* router, maka penulis memasukkan DNS yang berbeda dari DNS jaringan simulasi, sehingga apabila *client* mendapatkan IP *untrusted* maka *client* dan server dalam jaringan tidak mampu mentranslasikan DNS dan tidak terkoneksi ke server jaringan simulasi resmi perusahaan.

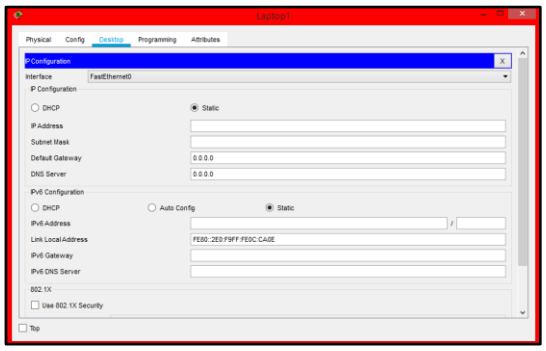
4.2 Tahapan pengetesan jaringan simulasi menggunakan metode Penetration Testing

Pada tahap ini, penulis akan mengetes jaringan dengan menggunakan tahapan *penetration testing*. Awal tahap akan dilakukan *planning* dengan menganalisa skenario dalam jaringan simulasi, kemudian tahap *information gathering* dengan mengumpulkan data informasi seputar jaringan simulasi seperti berapa banyak total *hardware* yang ada dalam jaringan, *IP*, *gateway* utama melalui mana. Kemudian dilanjutkan ke tahap *discovering vulnerabilities* yang mengindikasi celah keamanan jaringan. Seperti yang diketahui, jaringan simulasi tidak memiliki sistem keamanan sama sekali, sehingga apabila terdapat 2 DHCP server dalam jaringan simulasi akan terjadi pencemaran IP dari 2 server yang berbeda. Dan salah satunya berasal dari perusak jaringan. Apabila *client* mendapatkan IP dari perusak. Maka pihak tidak bertanggung jawab dapat mengendus trafik yang dilalui. Tahap exploit akan dijelaskan dalam subbab selanjutnya.

4.2.1 Pengetesan IP Yang diterima Client (exploit tanpa DHCP Snooping)

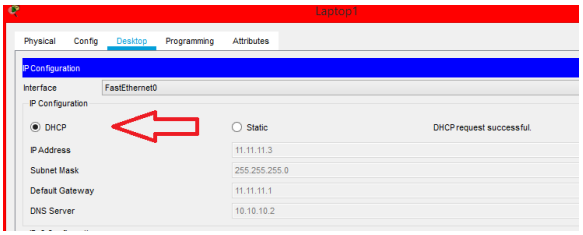
Pada tahap ini, penulis akan melakukan *request* IP DHCP dari *client*, setelah melakukan *request* dan berhasil mendapatkan IP, penulis akan melakukan pencatatan hasil IP yang didapat dari tiap komputer *client* dalam jaringan simulasi tanpa menggunakan keamanan *DHCP Snooping*. Langkah *request* IP akan dijelaskan penulis antara lain sebagai berikut:

1) Klik satu kali pada bagian komputer *client*, maka akan muncul jendela baru, pilih tab "*IP Configuration*", maka akan muncul jendela baru seperti pada Gambar 16:



Gambar 16 : Tampilan Jendela Baru IP Configuration

2) Ubah posisi "*Static*" menjadi "DHCP" untuk me*request* IP *DHCP server*. Maka hasil akhir akan terlihat seperti Gambar 17:



Gambar 17 : Request IP DHCP server

3) Penulis akan mengulangi langkah seperti yang tertulis di atas untuk melakukan pencatatan IP yang didapat oleh seluruh *client* jaringan simulasi. Dan hasilnya penulis sajikan pada Tabel 2 di bawah sebagai berikut:

Tabel 2

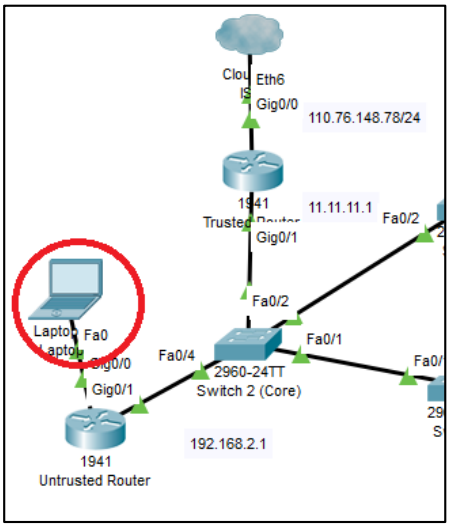
Pencatatan Hasil Request IP DHCP server dari Client

No	Perangkat	IP	Subnet	DNS	Gateway
1	PC 1	11.11.11.11	255.255.255.0	8.8.8.8	11.11.11.1
2	PC 2	192.168.2.24	255.255.255.0	8.8.8.8	11.11.11.1
3	PC 3	192.168.2.3	255.255.255.0	8.8.8.8	11.11.11.1
4	PC 4	11.11.11.15	255.255.255.0	8.8.8.8	11.11.11.1
5	PC 5	11.11.11.16	255.255.255.0	8.8.8.8	11.11.11.1
6	PC 6	11.11.11.17	255.255.255.0	8.8.8.8	11.11.11.1
7	PC 7	11.11.11.18	255.255.255.0	8.8.8.8	11.11.11.1
8	PC 8	11.11.11.19	255.255.255.0	8.8.8.8	11.11.11.1
9	PC 9	192.168.2.19	255.255.255.0	8.8.8.8	11.11.11.1
10	PC 10	11.11.11.22	255.255.255.0	8.8.8.8	11.11.11.1

4) Dari hasil yang penulis dapatkan, dari total 3 *client* yang melakukan *request* IP hanya 7 *client* yang mendapat IP *network* 11.11.11.0/24 yang merupakan jaringna resmi perusahaan, dan 3 *client* lainnya tidak mendapatkan IP resmi dari server perusahaan (192.168.2.0/24). IP tidak sesuai dengan jaringan perusahaan namun dengan ISP yang terhubung dan default gateway yang telah disetting dalam router trusted menyebabkan client tidak memiliki pengaruh apapun seperti jaringan down atau tidak terhubung internet, hanya saja client memiliki IP yang sama dengan peretas. Hal ini menyebabkan peretas mampu sniffing dan mengumpulkan informasi apapun yang berharga dalam trafik jaringan perusahaan.

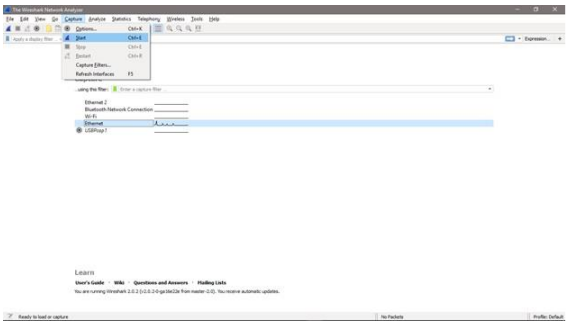
4.2.2 Dampak Client mendapat IP yang berbeda dengan jaringan perusahaan

Pada subbab ini, penulis akan menjelaskan bagaimana cara pencuri data jaringan mencuri dengan menggunakan DHCP Rogue. Yang dibutuhkan hanyalah perangkat lunak wireshark dan pastikan terhubung dengan jaringan target. Posisi pencuri jaringan berada pada posisi seperti pada Gambar 18 sebagai berikut:



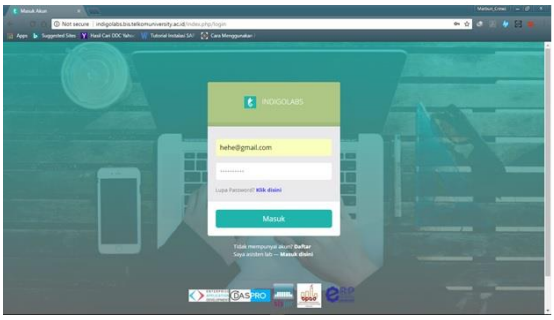
Gambar 18 : Skenario Posisi pencuri data

Pada laptop ini akan diinstall wireshark dan pastikan terhubung dengan jaringan. Tekan start untuk mulai sniffing packet yang teralir dalam jaringan (*Lihat Gambar 19*).



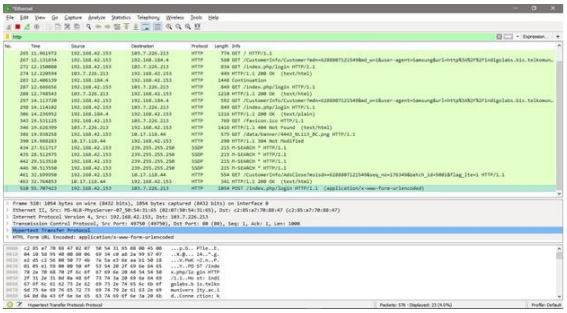
Gambar 19: mulai merekam aktivitas dengan wireshark

Setelah itu, pencuri tinggal menunggu aktivitas client untuk memasukkan data penting yang diakses dalam situs. Sebagai contoh apabila client mengakses situs yang membutuhkan login data, maka data yang diinput client untuk login akan terekam dalam wireshark (*Lihat Gambar 20*).



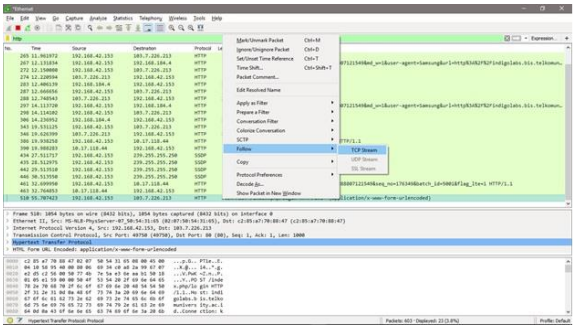
Gambar 20: Login situs client (Tampilan Client)

Agar pencuri data mudah menemukan jalur trafik tersebut, isi bagian filter dengan http dan kemudian pada bagian info jaringan cari dengan kata kunci POST (alamat yang dikunjungi dengan menggunakan sistemasi login) seperti pada Gambar 21 sebagai berikut:



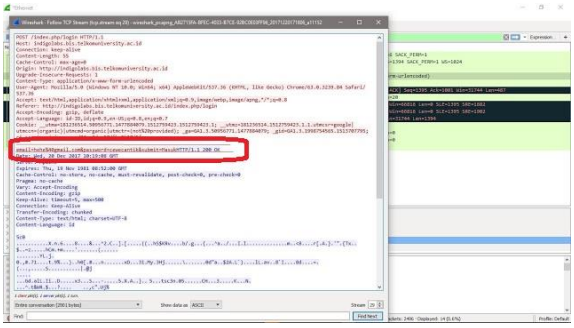
Gambar 21 : Login situs client (Tampilan pencuri Jaringan)

Setelah itu, klik kanan list trafik yang memiliki tulisan POST dan tekan follow, setelah itu tekan TCP Stream (Lihat Gambar 22).



Gambar 22 : Langkah mengikuti jejak trafik

Apabila langkah diatas telah selesai dilakukan, maka pencuri data tinggal menunggu client memasukkan data login, dan otomatis terekam dalam trafik wireshark (*ditunjukkan dalam Gambar 23*).



Gambar 23 : Hasil rekaman Data login wireshark

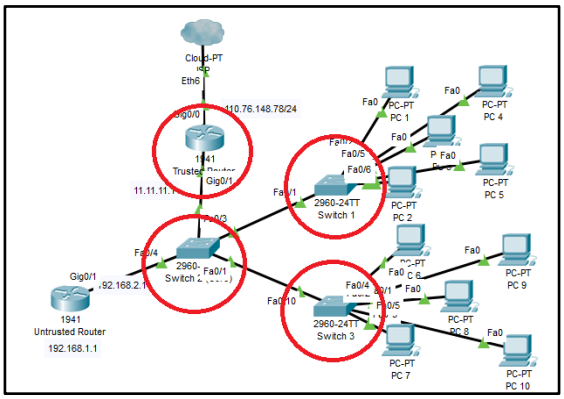
Dari skenario diatas, penulis menggambarkan betapa pentingnya keamanan jaringan bagi pengguna jaringan, karena dari cara sederhana diatas, mampu mencuri data penting perusahaan. Bayangkan apabila situs yang dituju merupakan situs perbankan atau situs privat untuk karyawan perusahaan. Dari cara tersebut, pihak yang tidak berwenang akan masuk ke dalam jaringan perusahaan dan mencuri data ataupun melumpuhkan jaringan perusahaan.

Untuk itulah dibutuhkan DHCP Snooping, akar masalah diatas dapat terjadi

karena pencuri data jaringan memiliki akses ke jaringan perusahaan dengan mencemari IP perusahaan dengan DHCP Rogue dimana pihak tidak berwenang membuat sebuah DHCP server duplikat dan menyebarkan IP dari pencuri data, sehingga IP peretas dengan target jaringan menjadi satu jaringan yang sama apabila client mendapat IP dari server pencuri data, alhasil mampu merekam aktivitas trafik client. DHCP snooping mampu memblokir jalur masuk pihak yang tidak dikenal jaringan perusahaan sehingga masalah yang disebutkan diatas tidak akan terjadi, karena jaringan hanya mengenal 1 *DHCP server* perusahaan, sehingga apabila ada server lain yang masuk, maka port tersebut akan otomatis mati.

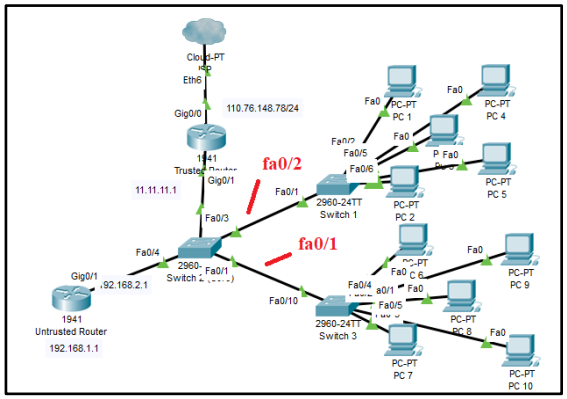
4.2.3 Konfigurasi Core Switch dengan DHCP Snooping

Pada tahap ini, penulis menggunakan jaringan simulasi yang sama, namun dengan tambahan fitur keamanan berupa DHCP *snooping* yang akan dikonfigurasi dalam router *trusted, core* switch, serta switch 1 & 2 dengan menyamakan VLAN, dalam posisi yang ditunjukkan pada Gambar 24 berikut:



Gambar 24 : Posisi Core Switch & router Trusted

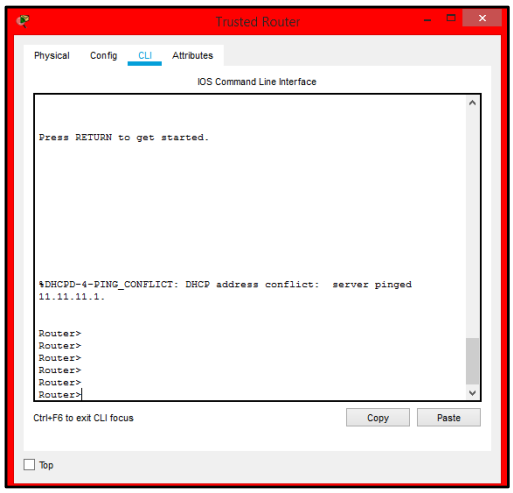
Tujuan dikonfigurasi pada switch dan router untuk mendaftar jalur yang hanya akan diterima switch jaringan. Dalam kasus ini, port yang akan penulis daftar sehingga terlabel "*trusted*" ialah port fa0/1, fa0/2 seperti yang ditunjukkan dalam Gambar 25 sebagai berikut:



Gambar 25 : Posisi trusted port yang akan dikonfigurasi

Penulis melakukan konfigurasi dengan langkah-langkah sebagai berikut:

1) Langkah pertama, penulis mengkonfigurasi DHCP server (*router trusted*). Klik gambar router maka akan muncul jendela baru, kemudian pilih tab CLI sehingga berada dalam posisi seperti Gambar 26:



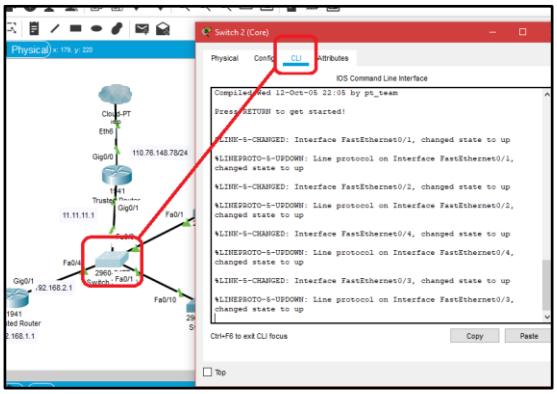
Gambar 26 : Jendela CLI

2) Langkah kedua penulis memasukkan beberapa perintah (*Command Line*) ke dalam seperti yang dituliskan dalam Gambar 27:

```
1 = Router(config)#ip dhcp relay information trust-all
2 = Router(config)#do wr
```

Gambar 27 : perintah DHCP Snooping Router

3) Pastikan router sudah terdapat konfigurasi *DHCP server* sebelumnya untuk melanjutkan memasukkan perintah pada Gambar 4.24. Fungsi darido w barisan 1 untuk mengaktifkan fitur DHCP *Snooping* dan mendaftarkan router tersebut sebagai sumber *DHCP server* yang terpercaya, kemudian barisan 2 untuk menyimpan konfigurasi.
4) Setelah selesai, penulis menutup jendela CLI tersebut dan beralih konfigurasi *core* switch, tekan gambar *core* switch dan pilih tab CLI seperti yang ditunjukkan Gambar 28:



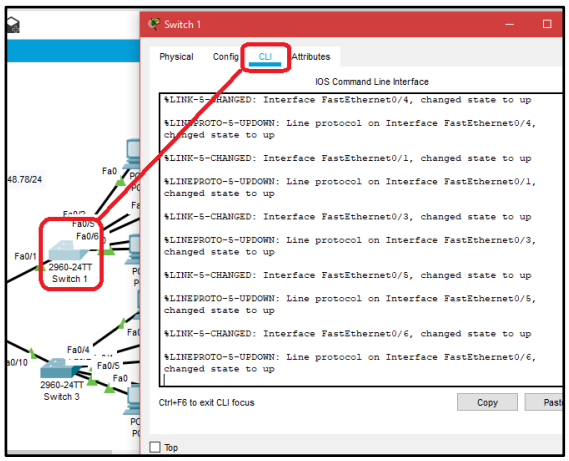
Gambar 28 : Konfigurasi Core Switch

5) Langkah selanjutnya penulis memasukkan beberapa perintah (*Command Line*) ke dalam seperti yang dituliskan dalam Gambar 29:

```
1 =  Switch>en
2 =  Switch#conf t
3 =  Switch(config)#vlan 10
4 =  Switch(config-vlan)#name dhcp_snooping
5 =  Switch(config)#int range fa0/1-24
6 =  Switch(config-if-range)#switchport mode access
7 =  Switch(config-if-range)#switchport access vlan 10
8 =  Switch(config-if-range)#end
9 =  Switch#conf t
10 = Switch(config)#ip dhcp snooping vlan 10
11 = Switch(config)#int fa0/1
12 = Switch(config-if)#ip dhcp snooping trust
13 = Switch(config)#int fa0/2
12 = Switch(config-if)#ip dhcp snooping trust
13 = Switch(config-if)#do wr
```

Gambar 29 : Konfigurasi DHCP Snooping pada core Switch

6) (*Lihat Gambar 29*) Pada nomor 1 & 2 merupakan langkah supaya penulis mampu masuk ke posisi *globalconfig mode* sehingga memiliki hak akses untuk mengkonfigurasi switch, nomor 3 memiliki fungsi untuk pendaftaran nomor VLAN baru yang awal mulanya default VLAN 1. Nomor 4 untuk pemberian nama pada VLAN dengan nama "*dhcp_snooping*". Nomor 5, 6 & 7 untuk pendaftaran seluruh port switch untuk masuk ke VLAN 10 dengan mode *access.* Nomor 8 untuk mengakhiri proses konfigurasi dan masuk kembali ke *user mode.* Nomor 9 untuk masuk kembali ke *globalconfig mode*. Nomor 10 untuk mengaktifkan fitur DHCP *snooping* dalam switch dan mendaftarkan fitur tersebut ke dalam vlan 10. Nomor 11 & 12 untuk mendaftarkan port fa0/1 dengan label "*trusted*" sehingga dapat dilalui oleh DHCP server. Nomor 13 & 14 untuk mendaftarkan port fa0/2 dengan label "*trusted*" sehingga dapat dilalui oleh DHCP server.
7) Setelah selesai beralih ke switch 1, tekan gambar switch 1 dan pada jendela baru yang muncul pilih tab CLI seperti yang ditunjukkan Gambar 30 sebagai berikut:



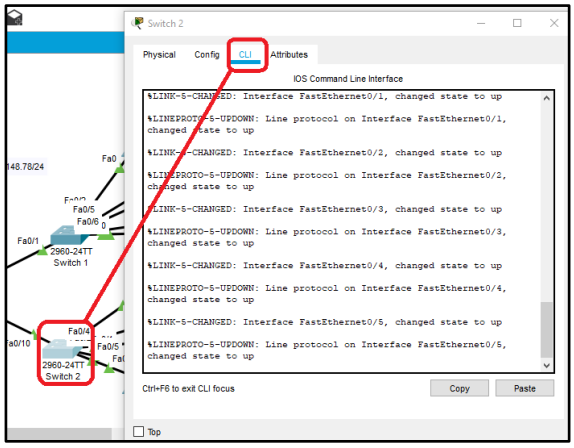
Gambar 30 : Konfigurasi switch 1

8) Langkah selanjutnya penulis memasukkan beberapa perintah (*Command Line*) ke dalam seperti yang dituliskan dalam Gambar 31:

```
1 =  Switch>en
2 =  Switch#conf t
3 =  Switch(config)#vlan 10
4 =  Switch(config-vlan)#name dhcp_snooping
5 =  Switch(config)#int range fa0/1-24
6 =  Switch(config-if-range)#switchport mode access
7 =  Switch(config-if-range)#switchport access vlan 10
8 =  Switch(config-if-range)#end
9 =  Switch#conf t
10 = Switch(config)#ip dhcp snooping vlan 1
11 = Switch(config)#int fa0/1
12 = Switch(config-if)#ip dhcp snooping trust
```

Gambar 31 : Perintah konfigurasi switch 1

9) (*Lihat Gambar 31*) Pada nomor 1 & 2 merupakan langkah supaya penulis mampu masuk ke posisi *globalconfig mode* sehingga memiliki hak akses untuk mengkonfigurasi switch, nomor 3 memiliki fungsi untuk pendaftaran nomor VLAN baru yang awal mulanya default VLAN 1. Nomor 4 untuk pemberian nama pada VLAN dengan nama "*dhcp_snooping*". Nomor 5, 6 & 7 untuk merubah VLAN yang semula semuanya VLAN 1 menjadi VLAN 10 dan dengan mode *access.* Nomor 8 untuk mengakhiri proses konfigurasi dan masuk kembali ke *user mode.* Nomor 9 untuk masuk kembali ke *globalconfig mode*. Nomor 10 untuk mengaktifkan fitur DHCP *snooping* dalam switch dan mendaftarkan fitur tersebut ke dalam VLAN 10. Nomor 11 & 12 untuk mendaftarkan port fa0/1 dengan label "*trusted*" sehingga dapat dilalui oleh *DHCP server* yang berstatus *trusted*. Port selain fa0/1 tidak memiliki keamanan *DHCP snooping* apabila tidak didaftarkan seperti langkah sebelumnya.
10) Setelah selesai tutup jendela CLI dan beralih ke switch 2, buka jendela konfigurasi dan pilih tab CLI seperti yang ditunjukkan pada Gambar 32 sebagai berikut:



Gambar 32 : Konfigurasi Switch 2

11) Langkah selanjutnya penulis memasukkan beberapa perintah (*Command Line*) ke dalam seperti yang dituliskan dalam Gambar 33:

```
1 =  Switch>en
2 =  Switch#conf t
3 =  Switch(config)#vlan 10
4 =  Switch(config-vlan)#name dhcp_snooping
5 =  Switch(config)#int range fa0/1-24
6 =  Switch(config-if-range)#switchport mode access
7 =  Switch(config-if-range)#switchport access vlan 10
8 =  Switch(config-if-range)#end
9 =  Switch#conf t
10 = Switch(config)#ip dhcp snooping vlan 1
11 = Switch(config)#int fa0/2
12 = Switch(config-if)#ip dhcp snooping trust
13 = Switch(config-if)#do wr
```

Gambar 33 : Perintah konfigurasi switch 2

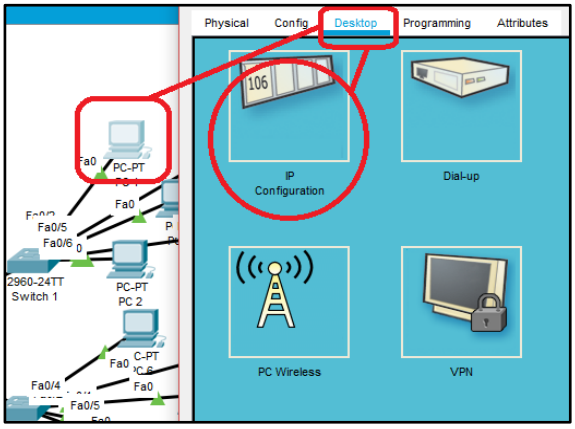
12) (Lihat Gambar 33) Pada nomor 1 & 2 merupakan langkah supaya penulis mampu masuk ke posisi *globalconfig mode* sehingga memiliki hak akses untuk mengkonfigurasi switch, nomor 3 memiliki fungsi untuk pendaftaran nomor VLAN baru yang awal mulanya default VLAN 1. Nomor 4 untuk pemberian nama pada VLAN dengan nama "*dhcp_snooping*". Nomor 5, 6 & 7 untuk merubah VLAN yang semula semuanya VLAN 1 menjadi VLAN 10 dan dengan mode *access.* Nomor 8 untuk mengakhiri proses konfigurasi dan masuk kembali ke *user mode.* Nomor 9 untuk masuk kembali ke *globalconfig mode*. Nomor 10 untuk mengaktifkan fitur DHCP *snooping* dalam switch dan

mendaftarkan fitur tersebut ke dalam VLAN 10. Nomor 11 & 12 untuk mendaftarkan port fa0/2 dengan label "*trusted*" sehingga dapat dilalui oleh *DHCP server* yang berstatus *trusted*. Port selain fa0/2 tidak memiliki keamanan *DHCP snooping* apabila tidak didaftarkan seperti langkah sebelumnya. Nomor 13 untuk menyimpan konfigurasi.

4.2.4 Pengetesan ulang IP Yang diterima Client (exploit tahap 2 dengan DHCP Snooping)

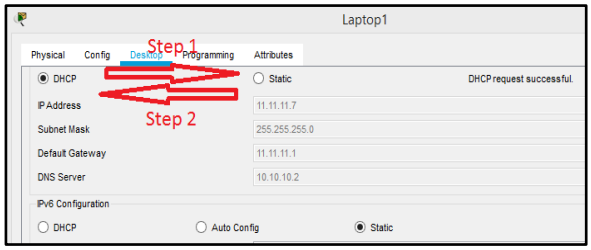
Setelah jaringan simulasi diterapkan keamanan *DHCP Snooping*, penulis akan mencatat ulang hasil *request* IP *DHCP client*, langkah-langkah yang diterapkan sebagai berikut:

1) Klik satu kali pada bagian komputer *client*, maka akan muncul jendela baru, pilih tab "*desktop*" kemudian tekan bagian "*IP Configuration*", maka akan muncul jendela baru seperti pada Gambar 34:



Gambar 34 : Jendela konfigurasi IP Client

2) *Request* IP DHCP ulang dengan mengubah posisi DHCP menjadi *static* kemudian ubah kembali lagi menjadi DHCP, sehingga IP yang didapat berbeda (Lihat Gambar 35):



Gambar 35 : Request ulang IP DHCP

3) Penulis mengulang langkah yang sama dengan di atas hingga semua *Client request* ulang IP, dan hasil IP yang diterima oleh *client* penulis rangkum dalam Tabel 3 di bawah:

Tabel 3

Pencatatan Hasil Request IP DHCP server dari Client

No	Perangkat	IP	Subnet	DNS	Gateway
1	PC 1	11.11.11.3	255.255.255.0	8.8.8.8	11.11.11.1
2	PC 2	11.11.11.7	255.255.255.0	8.8.8.8	11.11.11.1
3	PC 3	11.11.11.9	255.255.255.0	8.8.8.8	11.11.11.1
4	PC 4	11.11.11.10	255.255.255.0	8.8.8.8	11.11.11.1
5	PC 5	11.11.11.11	255.255.255.0	8.8.8.8	11.11.11.1
6	PC 6	11.11.11.4	255.255.255.0	8.8.8.8	11.11.11.1
7	PC 7	11.11.11.2	255.255.255.0	8.8.8.8	11.11.11.1
8	PC 8	11.11.11.8	255.255.255.0	8.8.8.8	11.11.11.1
9	PC 9	11.11.11.6	255.255.255.0	8.8.8.8	11.11.11.1
10	PC 10	11.11.11.5	255.255.255.0	8.8.8.8	11.11.11.1

4) Dari hasil rangkuman berupa tabel di atas, penulis mendapatkan hasil dimana 10 perangkat *client* mendapatkan IP resmi perusahaan.

4.3 Analisa DHCP Snooping & Perbandingan IP Client

Dari hasil penelitian yang telah penulis terapkan dalam jaringan simulasi, penerapan keamanan *DHCP Snooping* mampu membendung server DHCP lainnya yang tidak terdaftar dalam *server DHCP* resmi perusahaan. Ini dibuktikan dengan hasil IP *client* yang didapat penulis, penulis lampirkan perbandingan IP *client* sebelum dan sesudah penerapan keamanan *DHCP Snooping* pada Tabel 4 sebagai berikut:

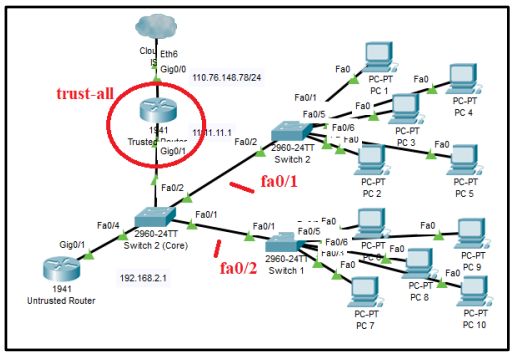
Tabel 4

Perbandingan IP Client sebelum dan sesudah penerapan keamanan DHCP Snooping

No	Sebelum	
	Perangkat	**IP**
1	PC 1	11.11.11.11
2	PC 2	192.168.2.24
3	PC 3	192.168.2.3
4	PC 4	11.11.11.15
5	PC 5	11.11.11.16
6	PC 6	11.11.11.17
7	PC 7	11.11.11.18
8	PC 8	11.11.11.19
9	PC 9	192.168.2.19
10	PC 10	11.11.11.22
No	**Sesudah**	
	Perangkat	**IP**
1	PC 1	11.11.11.3
2	PC 2	11.11.11.7
3	PC 3	11.11.11.9
4	PC 4	11.11.11.10
5	PC 5	11.11.11.11
6	PC 6	11.11.11.4
7	PC 7	11.11.11.2
8	PC 8	11.11.11.8
9	PC 9	11.11.11.6
10	PC 10	11.11.11.5

Berdasarkan tabel diatas, membuktikan bahwa pengaruh *DHCP Snooping* mampu membendung server DHCP lain yang memiliki jaringan yang berbeda, baik disengaja (*DHCP Server* yang berbeda untuk tujuan meretas jaringan) maupun tidak disengaja (kesalahan konfigurasi jaringan seperti *DHCP server* duplikat).

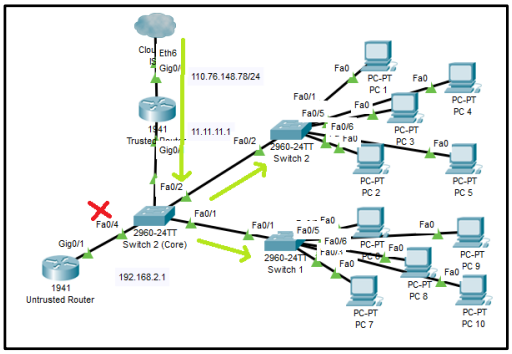
Cara kerja *DHCP snooping* berdasarkan analisa penulis dari hasil konfigurasi bahwa diharuskan mendaftar "jalur" yang terpercaya sehingga jalur tersebut dikenal oleh *DHCP server* untuk dilewati. Dalam jaringan simulasi penulis, jalur yang terpercaya yang terdiri dari port fa0/1 dan port fa0/2 pada posisi yang ditunjukkan Gambar 36, didaftarkan dalam konfigurasi switch *core* sebagai jalur terpercaya dan selain dari jalur itu, tidak akan dikenali atau port lain otomatis terputus. Penulis juga mengkonfigurasi router yang terpercaya dengan perintah "*trust-all*" untuk mendaftarkan router yang terpercaya sehingga dikenali sistem.



Gambar 36 : Posisi jalur terpercaya

Alasan *DHCP Snooping* diatur pada konfigurasi switch karena router hanya memiliki 2 port yang berfungsi dan seluruh port telah digunakan untuk keperluan koneksi jaringan, router dikonfigurasi hanya dengan perintah "*trust-all*" sehingga paket yang dikirim dari router tersebut akan dikenali sebagai sumber yang *trusted*. Sedangkan switch memiliki banyak port kosong, apabila tidak digunakan, menjadi salah satu jalan bagi perusak jaringan untuk terhubung melalui switch. Apabila tidak memiliki *DHCP snooping* menyebabkan pihak perusak jaringan dengan mudah masuk tanpa perlu konfigurasi apapun. Apabila perusak berhasil masuk, menyebabkan IP yang di*request* oleh *client* berbeda dengan *DHCP server* resmi perusahaan, menyebabkan *client* tidak mampu terhubung dengan server jaringan.

Apabila jaringan diterapkan keamanan *DHCP snooping*, maka *client* akan menerima IP resmi perusahaan karena jalur yang terpercaya telah terdaftar dalam *switch* sebelumnya. Sehingga secara logika, cara jalan paket IP yang berada dalam *DHCP server*, ketika akan dibagikan untuk *client* akan terlihat seperti ilustrasi pada Gambar 37 sebagai berikut:



Gambar 37 : Ilustrasi Cara jalan DHCP Snooping

5. Kesimpulan

Dari hasil penelitian yang telah penulis terapkan dalam jaringan simulasi, penulis dapat menyimpulkan dan menghasilkan jawaban atas rumusan masalah yang telah dibahas dalam bab 1 karya ilmiah mengenai bagaimana menerapkan keamanan jaringan, yaitu dengan menerapkan keamanan jaringan *DHCP Snooping* sehingga mampu terhindar dari *DHCP Rogue*, dimana cara kerjanya dengan pendaftaran jalur penyebaran *IP DHCP Server* resmi perusahaan telah diatur dan ditetapkan sebelumnya, dan menutup port jalur lain yang tidak digunakan, agar tidak menjadi celah keamanan untuk digunakan oleh pihak yang tidak bertanggung jawab guna merusak jaringan. Selain itu juga mampu menghindari kesalahan konfigurasi dari pihak yang berwenang.

5.1 Saran

Penelitian keamanan jaringan *DHCP Snooping* yang penulis buat terdapat beberapa keterbatasan dalam hal pembahasan. Dari keterbatasan ini, dapat penulis jadikan rekomendasi kepada penulis lain untuk pengembangan lebih lanjut dari penelitian ini. Keterbatasan yang dapat dijadikan rekomendasi untuk peneliti lainnya penulis rangkum sebagai berikut:

1) Penelitian yang dibahas berbasis *Cisco*, namun *DHCP Snooping* juga mampu dikonfigurasi dalam perangkat mikrotik dengan cara konfigurasi dan cara kerja yang berbeda. Alasan penulis tidak membahas konfigurasi perangkat mikrotik karena penulis ingin fokus dan konsisten dalam penanganan masalah keamanan jaringan yang berbasis *Cisco*, serta dari penelitian sebelumnya yang penulis bahas dalam bab 2, karya ilmiah yang membahas keamanan *DHCP Snooping* terlalu singkat dan banyak informasi penting yang tidak tercantum dalam penelitian penulis sebelumnya. Dengan alasan itulah penulis membahas topik *DHCP Snooping* berbasis *Cisco* dengan mencantumkan informasi penting sehingga karya ilmiah yang dihasilkan akan lebih bermanfaat bagi pembaca. Saran bagi penerus penelitian dari karya ilmiah penulis dengan menjelaskan konfigurasi *DHCP Snooping* berbasis mikrotik dan membahas kelebihan serta kelemahan dari masing-masing basis tersebut.
2) Disarankan untuk peneliti selanjutnya dengan menerangkan beberapa serangan *DHCP Server* lain yang telah penulis sebutkan dalam bab 2 dan bagaimana cara menangkalnya, karena untuk karya ilmiah yang penulis buat hanya membahas mengenai serangan *DHCP Rogue* dengan alasan keterbatasan waktu dan sumber daya.

DAFTAR PUSTAKA

Ariyadi, T. (2017). Desain Keamanan DHCP Snooping Untuk Mengurangi Serangan Local Area Network (LAN). *Jusikom*, *2*(1), 28–36.

Bohdanowicz, F., & Henke, C. (2014). Loop detection and automated route aggregation in distance vector routing. *Proceedings - International Symposium on Computers and Communications*, *0*(0), 1–6. https://doi.org/10.1109/ISCC.2014.6912454

Chen, X., & Mao, Z. (2015). Study on Availability and Security of DHCP System In Campus Network.

International Conference on Electronic Science and Automation Control (ESAC 2015), *1*(Esac), 44–47.

Cisco. (2016). Configuring DHCP Snooping. In *Cisco Nexus 5000 Series NX-OS Security Configuration Guide, Release 5.0(3)N1(1)* (Vol. 0, pp. 1–8).

Husni. (2014). Serangan ARP dan DHCP Pada Jaringan IPv4 dan IPv6. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *1*(23507026), 1–25.

Javid, S. R. (2014). Role of Packet Tracer in learning Computer Networks. *International Journal of Advanced Research in Computer and Communication Engineering*, *3*(5), 6508–6511.

Kadafi, M., & Kusnawi. (2015). ANALISIS ROGUE DHCP PACKETS MENGGUNAKAN WIRESHARK NETWORK PROTOCOL ANALYZER. *Journal of Applied Microbiology*, *119*(3), 1–6.

Khan, M., Alshomrani, E. S., & Qamar, S. (2013). Investigation of DHCP Packets using Wireshark. *International Journal of Computer Applications*, *63*(4), 975–8887. https://doi.org/10.5120/10451-5155

Kocaleva, M., Stojanovik, I., & Zdravev, Z. (2015). *International Conference on Information Technology and Development of Education Itro 2015 Informacione Tehnologije I Razvoj Obrazovanja Itro 2015*. *Research on Utaut Application in Higher Education Institutions*.

Miftah, Z. (2018). DESAIN KEAMANAN DHCP SNOOPING UNTUK MENGURANGI SERANGAN LOCAL AREA NETWORK(LAN). *Faktor_Exacta*, *11*(2), 167–178. https://doi.org/10.30998/faktorexacta.v11i2.2456

Muhammad, M., & Hasan, I. (2016). Analisa dan Pengembangan Jaringan Wireless Berbasis Mikrotik Router OS V . 5 . 20 di Sekolah Dasar Negeri 24 Palu. *Jurnal Elektronik Sistem Informasi Dan Komputer*, *2*(1), 10–19.

Putra, A. D. G., & Wiwin Sulistyo, S.T., M. K. (2014). Analisis dan Perancangan Jaringan VLAN Studi Kasus SMK Negeri 2 Salatiga. *Artikel Ilmiah*, *0*(672009076), 1–17.

Rizkilla, N. Z., M, R. R., & Mulyana, A. (2016). Perancangan dan Analisis Transmisi Video Live Streaming Melalui Wireless-LAN (WLAN) di Gedung P, Fakultas Teknik Elektro Univeritas Telkom. *E-Proceeding of Engineering*, *3*(3), 5036–5042.

Sari, H. L., Sudarsono, A., & Hayadi, H. (2013). Pengembangan Jaringan Local Area Network Menggunakan Sistem Operasi Linux REDHAT 9. *Jurnal Media Infotama*, *9*(1), 165–189.

Szeto, R. W., Jain, N., Suresh, R., & Kwan, P. (2013). SYSTEMAND METHOD FOR SOURCE IP ANTI-SPOOFING SECURITY. *Cisco (“Configuring Port-Based Traffic Control.” Catalyst 3550 Multilayer Switch Software Configuration Guide, Cisco IOS Release 12.1 (13) EA1, Mar. 2003, Pp. 1-48, Ch. 20 Cisco Systems, Inc.*, *2*(12), 1–25. https://doi.org/10.1038/incomms1464

Wu, K., Li, Y., Chen, L., & An, S. (2016). Research of DHCP Flooding Attack Detection Technology Based on Improved Wavelet Analysis Method. *Department of Control and Computer Engineering, North China Electric Power University, No.2 Beinong Road, Changping District, Beijing 102206, Beijing, China*, *9*, 294–308.